AUTORITÀ PER LE GARANZIE NELLE COMUNICAZIONI
AGCOM

**Allegato 3 alla delibera n. 68/21/CIR**

# SPECIFICHE PER IL SISTEMA DI CRIPTAGGIO DELLE INFORMAZIONI SENSIBILI DEI CLIENTI FINALI NELL'AMBITO DEL PROCESSO *WHOLESALE*DI *DELIVERY* DI TELECOM ITALIA S.P.A. AI SENSI DEL PUNTO 1), DELL'ALLEGATO B DELLA DELIBERA N. 420/19/CONS

# Indice

# Premessa

- L'impegno 1 dell'Allegato B della Delibera 420 19 CONS riporta:

  "*TIM si impegna ad individuare, entro 30 giorni dall'approvazione degli impegni, una soluzione tecnica che possa essere condivisa anche dagli OAO, che impedisca la visualizzazione di dati sensibili (nome e cognome cliente, CF/Partita IVA e recapito telefonico) in caso di qualunque operazione di estrazione singola o massiva di ordinativi da parte di qualunque personale autorizzato all'accesso tramite interfaccia grafica (GUI) al sistema, quindi outsourcers, personale TIM Wholesale e OAO. In proposito saranno create delle nuove profilature ad hoc per gli utenti dei sistemi, con diversi livelli autorizzativi di accesso e tracciamento degli stessi accessi, che permettano di visualizzare da interfaccia grafica i dati sensibili solo dal personale autorizzato, per la cui attività lavorativa è necessario accedere a queste informazioni, escludendo tale possibilità per tutti gli altri utenti dei sistemi. In logica di full equivalence la misura sarà estesa anche al caso di ordinativi retail TIM. In altri termini anche per gli ordinativi di TIM retail né agli outsourcers né il personale di TIM wholesale potrà estrarre i suddetti dati sensibili. Per quanto riguarda il sistema NOW, le modifiche proposte dovranno essere preventivamente concordate anche con gli OAO perché tale sistema viene utilizzato anche da personale OAO*".

- Il presente documento, con riferimento al processo di Delivery, riporta una soluzione tecnica basata sull'utilizzo dei token.

# Definizione delle informazioni sensibili

Nel presente documento per informazioni sensibili (di seguito dati sensibili) si intende l'insieme delle informazioni, riportate nella tabella seguente, dalle quali direttamente o indirettamente è possibile contattare il cliente dell'Operatore.

| **Informazioni sensibili** |
| --- |
| Nome cliente |
| Cognome cliente/Ragione sociale |
| CF/PIVA del cliente |
| Recapito telefonico del cliente |
| Eventuale recapito alternativo del cliente |

# Criptazione delle informazioni sensibili (1/4)

TIM svilupperà la soluzione di criptazione secondo le seguenti modalità:

1. TIM cripta i dati sensibili appena «entrano nei sistemi TIM».
2. Per le interfacce grafiche utente (c.d. GUI) dei sistemi acceduti dagli Operatori né l'OAO, né TIM avranno la possibilità di visualizzare in chiaro i dati sensibili.
3. La criptazione consiste nella sostituzione di ciascuno dei dati sensibili con un identificatore unico detto token.
4. Il token è memorizzato in un DB protetto che è esterno ai sistemi di delivery di TIM.
5. Il DB, corredato delle più recenti e innovative misure di sicurezza per garantire la riservatezza dei dati sensibili, conterrà l'associazione tra i dati sensibili del cliente e il token.
6. Sui sistemi di delivery i dati sensibili non saranno più presente in chiaro ma al loro posto sarà visualizzato il token.
7. Il DB non sarà dotato di accessi tramite GUI.
8. Il DB sarà interrogato in ottica *need to know* dai sistemi che utilizzeranno i dati criptati per l'esecuzione dell'ordine di provisioning.
   L'accesso al DB sarà permesso al solo personale IT che svolge attività di sviluppo ed esercizio del Sistema, per le analisi di sicurezza e per la gestione di eventi particolari, anche su liste di ordini, descritti nel successivo punto 13.

# Criptazione delle informazioni sensibili (2/4)

9. L'OAO non dovrà inserire nei campi Note dei tracciati record i dati sensibili. Qualora lo facesse, in assenza di misure di controllo riportate nel successivo punto 10, qualsiasi misura di profilatura rischierebbe di perdere la sua validità in quanto i dati sarebbero disponibili in chiaro sul campo Note.
10. TIM attuerà soluzioni di controllo per minimizzare la perdita di validità della criptazione dei dati sensibili nel caso in cui l'OAO dovesse inserire nel campo note **i recapiti telefonici**. In particolare su tale campo TIM utilizzerà algoritmi di pattern matching e di riconoscimento di sequenza di numeri con determinate caratteristiche per «intercettare» la presenza di eventuali numeri telefonici. Tutti i numeri telefonici intercettati dall'algoritmo, ivi inclusi eventuali riferimenti telefonici dell'OAO, verranno sovrascritti rendendoli inutilizzabili.
11. Di contro, TIM non effettuerà alcuna sovrascrittura di eventuali **dati anagrafici** del cliente inseriti dall'OAO nei campi Note. Qualora l'OAO inserisse impropriamente tali informazioni in tale campo queste rimarranno in chiaro.
12. I tecnici *on field* utilizzeranno i dati sensibili in fase di lavorazione dell'ordine di delivery, mediante detokenizzazione della sola anagrafica cliente, secondo le modalità riportate nelle slide seguenti «Focus su criptazione». Ciò per contattare il cliente al fine di confermare l'appuntamento preso durante la Policy di Contatto per realizzare il servizio presso la sede del cliente finale dell'OAO. Nel caso di Work Request (c.d. WR) relativa a clienti TIM, la detokenizzazione sarà automatica e, attraverso una piattaforma informatica, farà si che il cliente verrà messo in contatto con il tecnico tramite una chiamata che parte da numerazione specifica (es 187/191). Stessa procedura opzionale sarà resa disponibile per gli OAO che vorranno far contattare il proprio cliente dal proprio numero di Customer Care. Ovviamente ciò richiederà un apposito contratto tra TIM e l'OAO. In questo modo si da maggiore trasparenza al cliente dell'Operatore che lo sta contattando. Ciò sarà implementato anche per l'assurance.

# Criptazione delle informazioni sensibili (3/4)

13. In caso di richieste specifiche provenienti da enti esterni (es AGCOM, ODV,..), reclami, contenziosi, richieste di escalation, supporto ai tecnici *on field* per la gestione di eccezioni nel processo di delivery, gestione di richiamate o recuperi nel processo di presa appuntamento su ordine di delivery, i dati sensibili saranno rese disponibili, a personale ad hoc di TIM, tramite detokenizzazione.
14. Non sarà consentita all'OAO la visualizzazione «*on demand*» dei dati sensibili.
15. La soluzione di criptazione di TIM realizza una divisione netta sul reperimento dei dati sensibili a seguito dell'invio dell'ordine di provisioning da OAO a TIM: sui sistemi di TIM per TIM, sui sistemi OAO per OAO.
16. TIM invierà agli OAO, che inseriscono gli ordini di provisioning dei servizi wholesale via GUI, le notifiche previste nel processo di provisioning tramite file xml. Pertanto, la modalità di invio delle notifiche via xml, sostituirà quella di invio via email, ad oggi in essere per alcune tipologie di ordini di provisioning inseriti dagli OAO via GUI (es servizi BTS rame, BTS NGA e VULA). Per tutti gli OAO si dovrà configurare l'area SFTP.
17. Per i progetti speciali, identificati con codici progetto ad hoc, gli OAO dovranno riportate i propri referenti, che gestiscono il progetto speciale, nei campi referente presenti sui tracciati record dei servizi wholesale anziché nel campo Note. Ciò dovrà essere effettuato per tutti i servizi wholesale i cui tracciati contengono campi con dati sensibili (per esempio ciò non sarà necessario per i servizi di colocazione che non contengono dati sensibili). TIM introdurrà, nei tracciati record dei servizi wholesale, un nuovo campo opzionale per i soli progetti speciali in cui l'OAO potrà inserire una/più numerazioni telefoniche necessarie per l'esecuzione del progetto speciale stesso.

# Criptazione delle informazioni sensibili (4/4)

18. Al fine di permettere all'Operatore di inviare a TIM le informazioni relative al recapiti telefonici del cliente in campi strutturati, TIM inserirà i campi referente cliente in tutte le notifiche inviate dall'Operatore a TIM in cui attualmente non sono presenti, ma sono necessari per la lavorazione dell'ordine. Tali campi saranno opzionali. Verranno utilizzati i tag referenti già presenti nelle altre notifiche. Le notifiche oggetto di modifica sono riportate nella tabella seguente.

| Servizio wholesale | Nome notifica |
|---|---|
| ULL, SLU, | Rimodulazione appuntamento |
| Bitstream ATM e GBE Simmetrico e Asimmetrico | Rimodulazione Data Appuntamento |
| WLR | Rimodulazione appuntamento |
| Bitstream NGA VULA | Rimodulazione Data Appuntamento |
| Easy IP | Rimodulazione Data Appuntamento |

# Tracciamento degli accessi

## Tracciamento degli accessi al DB in cui è memorizzato il token

Tutti gli accessi ai dati sensibili detokenizzati verranno tracciati su log di sistema con indicazione dell'utente che ha effettuato l'accesso, dell'operazione svolta, del dato interrogato e della data di accesso.

# Altre misure (1/3)

1. Per il sistema NOW verrà inibita la possibilità di estrarre report massivi contenenti dati sensibili. I dati sensibili non saranno più resi disponibili per nessun profilo. Più in dettaglio, TIM:
   - manterrà la possibilità per gli OAO di effettuare estrazioni massive di ordini, secondo i profili di accesso assegnati
   - cripterà i soli dati sensibili
   - lascerà in chiaro le restanti informazioni.

1. In linea con quanto comunicato da TIM con news del 18 febbraio u.s.:
   - dal 16 marzo u.s, TIM ha introdotto la funzionalità **denominata "Blocco Multisessione"** che impedisce l'apertura di più di una sessione contemporanea nell'area privata del Portale Wholesale, da parte della stessa utenza
   - da febbraio u.s. è implementata e disponibile, su base richiesta dell'OAO, la funzionalità denominata **Implementazione Access Control List (ACL)** che permette per ciascuna delle utenze dell'OAO, su base elenco indirizzi IP di limitare l'accesso al Portale Wholesale ad un ristretto numero di indirizzi IP comunicati dall'OAO stesso. Più in dettaglio TIM effettua un controllo della corretta associazione tra account ed IP di provenienza: se l'account non è associato ad uno degli IP comunicati da OAO a TIM, TIM non consente l'accesso alla sezione riservata dell'Area Wholesale del Portale Wholesale ed ai sistemi acceduti tramite portale.

# Altre misure (2/3)

3. TIM cripterà i dati sensibili presenti nei file xml di notifica del processo di delivery disponibili sulle GUI di NOW. Ciò per evitare che i dati sensibili restino disponibili nei file di notifica.

   Pertanto i file di notifica xml continueranno ad essere disponibili per gli OAO:

   - con **i dati sensibili criptati** sulle GUI di NOW, mantenendo l'attuale formato.
   - con **i dati sensibili in chiaro** sul server SFTP, senza alcuna modifica.

4. TIM introdurrà nel tool di «Segnalazione di Provisioning» due campi specifici denominati «Riferimento telefonico» (max 128 caratteri) e «Indirizzo cliente» (max 128 caratteri), in cui gli OAO potranno inserire rispettivamente uno/più recapiti telefonici del cliente e l'indirizzo del cliente. I recapiti verranno inseriti dall'OAO in sequenza separati dai caratteri «;» oppure «/» oppure spazio. TIM provvederà a tokenizzare il campo «Riferimento telefonico». Il personale di TIM preposto alla lavorazione della segnalazione di provisioning, se necessario, potrà detokenizzare tale campo per la lavorazione della segnalazione stessa. Il campo **Indirizzo Cliente** sarà lasciato in chiaro. Eventuali recapiti telefonici inseriti dall'OAO nel campo Note verranno sovrascritti rendendoli inutilizzabili secondo quanto riportato al punto 10 delle slide «*Criptazione delle informazioni sensibili*». Il codice ordine non verrà criptato.

# Altre misure (3/3)

5. Per quanto riguarda l'Assurance, con riferimento ai c.d. «TT CX» e ai TT «CPS e NP», TIM modificherà il processo in essere, che prevede la sovrascrittura dei riferimenti telefonici per testare la corretta risoluzione del TT presenti nel campo Note, non effettuando tale sovrascrittura.

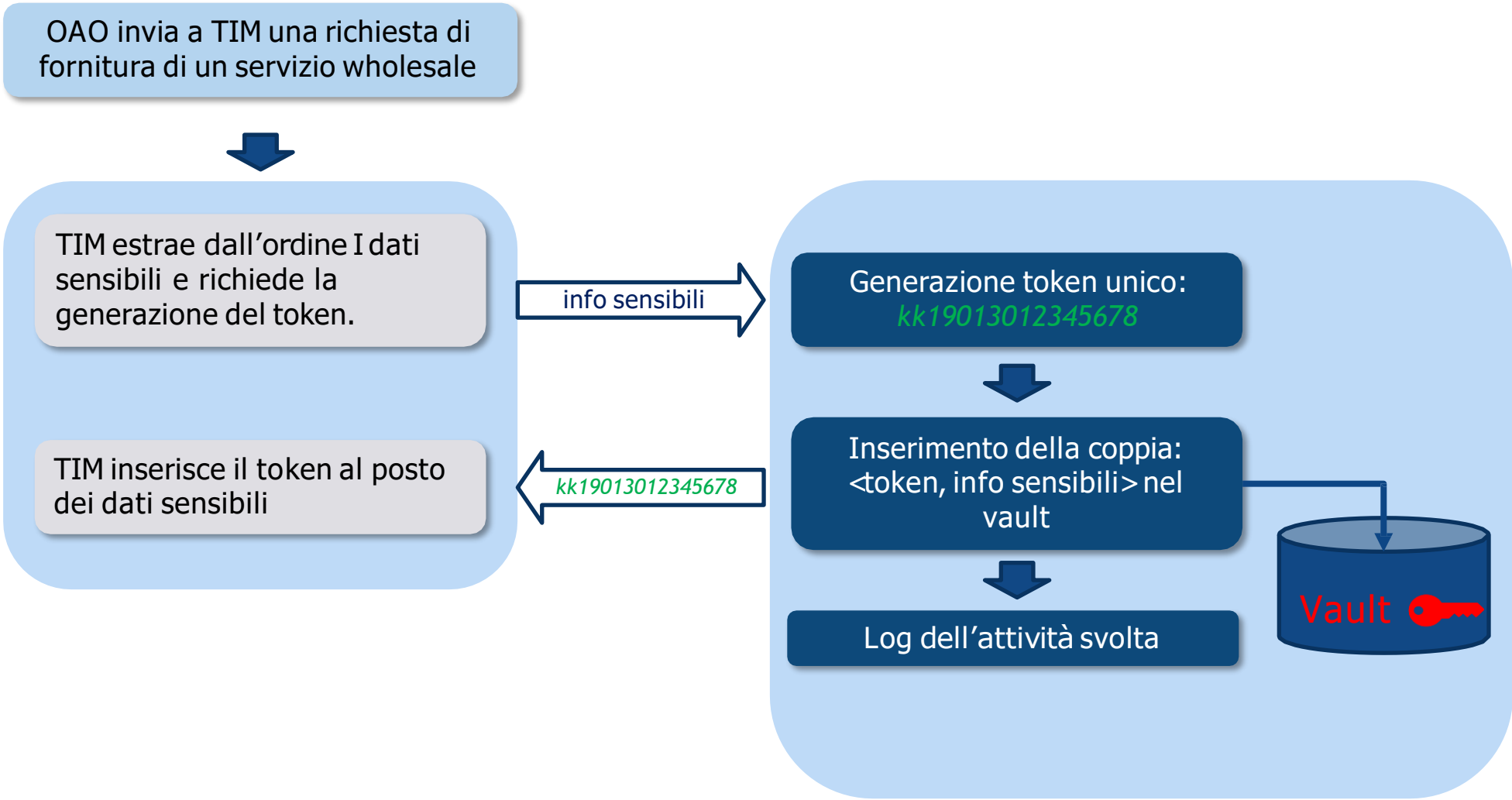
6. TIM introdurrà nella richiesta del «Quarto referente digitale- 4 APP» un campo specifico denominato "Riferimento telefonico" (max 128 caratteri) nel quale gli OAO potranno inserire uno/più recapiti telefonici del cliente. I recapiti verranno inseriti dall'OAO in sequenza separati dai caratteri «;» *oppure «/» oppure spazio.* TIM provvederà a tokenizzare tali recapiti che saranno gestiti dai tecnici on field (in ordine di inserimento) in fase di lavorazione dell'ordine di delivery secondo le modalità riportate nelle slide seguenti *« Focus su criptazione».* Eventuali recapiti telefonici inseriti dall'OAO nel campo Note verranno sovrascritti rendendoli inutilizzabili secondo quanto riportati al punto 10 delle slide «Criptazione delle informazioni sensibili».

# Fasi di progetto

**La criptazione delle informazioni sensibili** per il processo di delivery verrà sviluppata da TIM, a valle della relativa condivisione da parte degli OAO e di AGCom.

I **tempi di rilascio** in esercizio della soluzione informatica saranno valutati da TIM, in accordo con gli OAO e l'Autorità, a valle del consolidamento e dell'approvazione della soluzione descritta nel presente documento.

# Focus su criptazione: Generazione e gestione del token (1/2)



# Focus su criptazione: Generazione e gestione del token (2/2)

## Tecnici On Field (TIM ed Impresa)

I dati dell'anagrafica del cliente sono detokenizzati :

- sullo smartphone del tecnico on field TIM, al momento della lavorazione;
- sul sistema di assegnazione dell'Impresa, al momento dell'assegnazione della lavorazione (WR).

Il tecnico on field chiama il cliente con anagrafica del cliente in chiaro e recapiti telefonici tokenizzati.

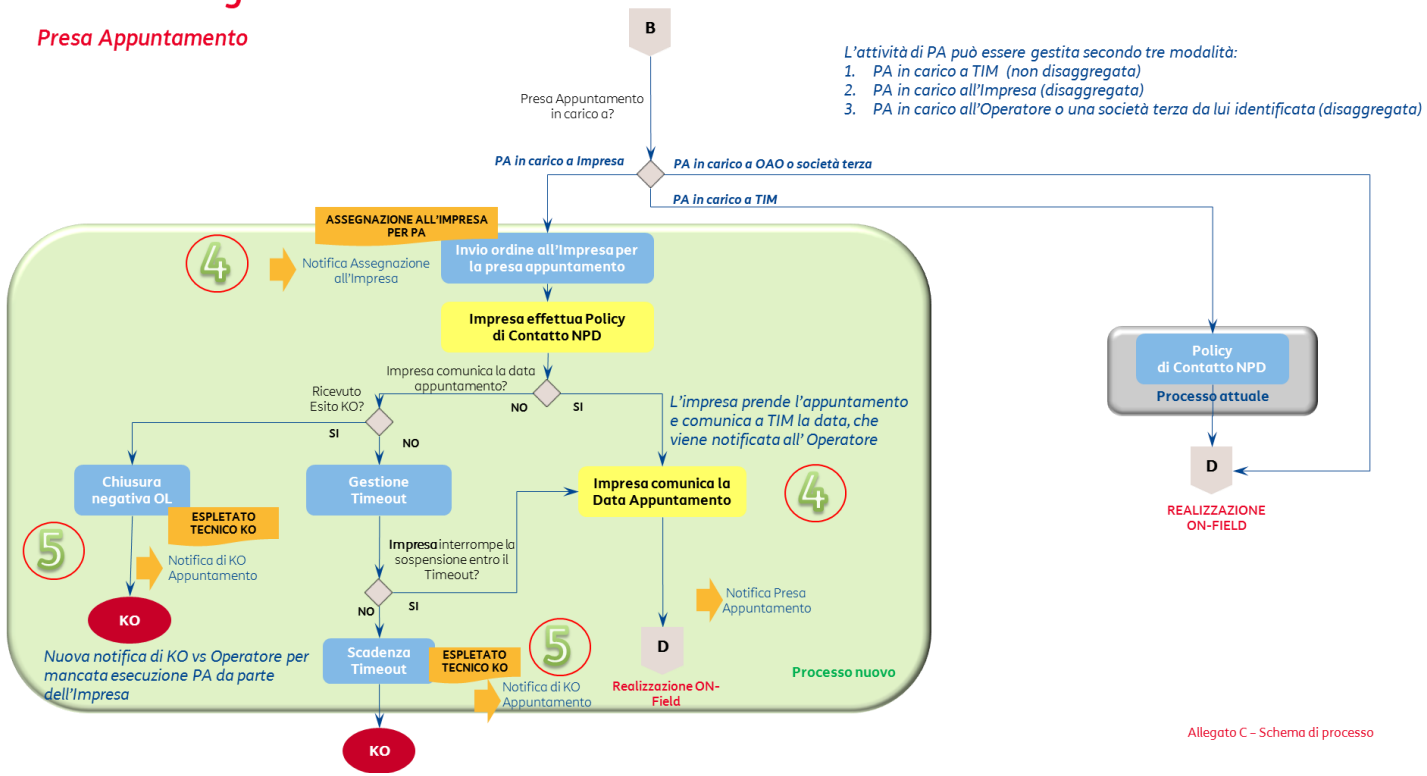
# Focus su gestione Presa Appuntamento in modalità disaggregata (1/4)

La gestione della Presa Appuntamento (**PA**) in modalità disaggregata è **in esercizio dal 23 luglio 2020 per l'ULL/SLU e dal 27 settembre per il VULA C e prevede che:**

la «*PA può essere gestita secondo tre modalità:*

- *PA in carico a TIM (**non disaggregata**)*
- *PA in carico all'Impresa (**disaggregata**)*
- *PA in carico all'Operatore o una società terza da lui identificata (**disaggregata**)»*

## Provisioning: attivazione LNA




Allegato C – Schema di processo

# Focus su gestione Presa Appuntamento in modalità disaggregata (2/4)

## PA in carico all'Operatore o ad una società terza da lui identificata

In caso di PA in carico all'Operatore o ad una società terza da lui identificata, l'introduzione della soluzione di criptazione dei dati sensibili non comporta alcuna necessità di revisione della soluzione disaggregata in campo. Ciò in quanto l'Operatore invia a TIM l'OL con la data di appuntamento già fissata che, non essendo un dato sensibile, viene inviata all'Impresa in chiaro.

## PA in carico all'IMPRESA

La soluzione di disaggregazione in campo e la soluzione di criptazione (riportata nel documento «Delibera 420/19/CONS Allegato B Impegno 1 Processo di Delivery» del 15 luglio 2020) prevedono

1. per la soluzione di disaggregazione, che l'ordine venga inoltrato all'impresa per l'effettuazione della PA.
2. per la soluzione di criptazione, che:
   *«I tecnici on field utilizzeranno i dati sensibili in fase di lavorazione dell'ordine di delivery, mediante detokenizzazione della sola anagrafica cliente, secondo le modalità riportate nelle slide seguenti «Focus su criptazione».* ***Ciò per contattare il cliente al fine di confermare l'appuntamento preso durante la Policy di Contatto per realizzare il servizio presso la sede del cliente finale dell'OAO….».***

La PA in carico all'Impresa potrà essere gestita secondo le due seguenti modalità:

| PA in carico all'IMPRESA – modalità A | PA in carico all'IMPRESA – modalità B |
|---|---|
| L'OAO comunica all'Impresa le informazioni sensibili necessarie per effettuare la PA. Sarà l'Impresa, ricevuto l'ordine disaggregato da TIM secondo le modalità attualmente in campo, a recuperare i dati sensibili comunicatigli dall'OAO per effettuare la PA. | L'Impresa utilizza le modalità descritte al punto 2, modificate da TIM secondo quanto riportato nelle due slide successive, al fine di effettuare anche la presa appuntamento. |

# Focus su gestione Presa Appuntamento in modalità disaggregata (3/4)

## PA in carico all'IMPRESA – modalità B

TIM adeguerà *l'applicazione già disegnata «**per contattare il cliente al fine di confermare l'appuntamento preso durante la Policy di Contatto per realizzare il servizio presso la sede del cliente finale dell'OAO**….» (di seguito **applicazione**)* in modo da permettere all'impresa di effettuare la chiamata al cliente per la PA in modalità disaggregata. In dettaglio TIM:

- abiliterà l'utilizzo dell'applicazione in caso di ordini di lavoro con PA disaggregata in carico ad Impresa;
- permetterà l'utilizzo dell'applicazione da PC o da tablet;
- fornirà la possibilità di abilitare all'utilizzo dell'applicazione utenze specifiche comunicate dall'Impresa a TIM;
- permetterà l'effettuazione del tentativo di chiamata a tutti i referenti del Cliente, in caso di mancata risposta da parte di uno o più recapiti;
- permetterà all'operatore dell'impresa, in fase di autenticazione, di inserire il numero telefonico che l'applicazione utilizzerà per metterlo in contatto con il cliente. Tale numero di telefono potrà essere una numerazione fissa, mobile o di un centralino che smisti automaticamente le chiamate tra più operatori (in tale ultimo caso a condizione che al numero in questione risponda direttamente un operatore esclusivamente dedicato alla PA, senza pertanto l'introduzione di IVR, toni di attesa, deviazioni di chiamata o rumore).
- metterà a disposizione una funzionalità che permetterà all'operatore dell'Impresa di inserire, in una finestra dell'applicazione, una lista di token. La piattaforma chiamerà in successione, su comando dell'operatore, i token da lui inseriti. All'atto della chiamata l'anagrafica del cliente (nome cognome/ragione sociale) sarà visualizzata in chiaro
- per gestire il maggior carico di chiamate contemporanee, potenzierà l'accesso:
  - al "DB protetto" che "*conterrà l'associazione tra i dati sensibili del cliente e il token*»
  - all'applicazione.

  Tale potenziamento sarà effettuato da TIM sulla base delle previsioni di volumi di chiamate al giorno e al numero massimo di chiamate per ora che ciascun OAO prevederà di gestire mediante la PA disaggregata a cura dell'impresa. Tale previsione sarà formita dagli OAO una volta condivisa la soluzione tecnica riportata nel presente documento prima dell'avvio dell'implementazione.

# Focus su gestione Presa Appuntamento in modalità disaggregata (4/4)

**PA in carico all'IMPRESA – modalità B**

**Applicazione per contattare il Cliente (da PC)**

L'operatore dell'Impresa che effettua la PA inserisce, in fase di autenticazione, sulla piattaforma:

- il numero in chiaro dell'utenza telefonica dell'operatore dell'Impresa
- la lista di token, o il singolo token, corrispondente ai recapiti dei clienti, o del singolo cliente, da contattare, presenti nelle «Work Request» inviate da TIM all'impresa

L'operatore seleziona un token corrispondente ad un cliente da chiamare

L'applicazione chiama il numero telefonico inserito dall'operatore dell'Impresa

Quando l'operatore risponde, la piattaforma inizia a contattare il primo recapito del cliente corrispondente al token selezionato. In caso di mancata risposta viene chiamato il recapito successivo fino all'esaurimento di tutti i recapiti Cliente inseriti nell'ordine dall'OAO

Quando il cliente risponde, la piattaforma effettua la connessione con l'addetto e la conversazione può avvenire

La piattaforma chiamerà in successione, su comando dell'operatore, i token da lui inseriti nella lista dei token, ovvero il singolo token.